UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	NO. 1:08CR239 (GBL)
	)	
ELAINE ROBERTSON CIONI	)	

MEMORANDUM IN SUPPORT OF DEFENDANT'S RULE 29 MOTION

COMES NOW the defendant, Elaine Robertson Cioni, by counsel, and submits the following memorandum in support of her Motion for Judgement of Acquittal pursuant to Rule 29 of the Federal Rules of Criminal Procedure.

I. THE EVIDENCE IS INSUFFICIENT TO ESTABLISH THAT THE DEFENDANT CONSPIRED WITH ANOTHER PERSON TO VIOLATE §1030(A)(2)(C) IN FURTHERANCE OF A VIOLATION OF § 2701.

The government offered no evidence of an agreement between the defendant and any other person to access protected computers owned by AOL or any other internet service provider and obtain emails. Nor did the government offer any evidence of an agreement between the defendant and any other person to do so in furtherance of the offense of accessing AOL or any other internet service provider to obtain unopened emails.

II. THE EVIDENCE ON COUNTS 1, 2 AND 4 IS INSUFFICIENT TO ESTABLISH THAT MS. CIONI VIOLATED §1030(A)(2)(C) IN FURTHERANCE OF A VIOLATION OF § 2701.

The government offered no evidence that the defendant acted with the intent or purpose to gain access to "unopened emails" – a necessary element of § 2701.

Section 2701 provides:

(a) **Offense**. – whoever–

> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
>
> (2) intentionally exceeds an authorization to access that facility;
>
> and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section . . .

The term "in electronic storage" is narrowly defined in 18 U.S.C. § 2510(17) and refers only to temporary storage, made in the course of transmission, by a provider of electronic communications service. If the communication has been accessed, i.e., opened, by a recipient, it is no longer in "electronic storage." *Fraser v. Nationwide Mutual Insurance Co.*, 135 F. Supp. 2d 623, 634-638 (E.D. Pa. 2001)

The government has offered no evidence that any of the emails that the defendant accessed or attempted to access had not be previously read (opened) by their intended recipients.

III. THE GOVERNMENT'S EVIDENCE IS INSUFFICIENT TO PROVE THAT THE DEFENDANT INTENTIONALLY ACCESSED, OR ATTEMPTED TO ACCESS A "PROTECTED COMPUTER" IN VIOLATION OF §1030(a)(2)(C)) OR AN "ELECTRONIC COMMUNICATIONS SERVICE" IN VIOLATION OF § 2701, IN THAT THE GOVERNMENT'S EVIDENCE FAILED TO ESTABLISH THAT THE DEFENDANT'S ACCESS OR ATTEMPTED ACCESS WAS WITHOUT AUTHORIZATION OR EXCEEDED AUTHORIZATION.

The government presented no evidence that Ms. Cioni's access or attempted access was not authorized by the owners of the "protected computers" and "electronic communications services," who are the internet service providers and not the email account holders.

IV. THE GOVERNMENT'S EVIDENCE IS INSUFFICIENT TO SUSTAIN A FELONY CONVICTIONS FOR COUNT 1 (CONSPIRACY TO VIOLATE 18 U.S.C. § 1030 (a)(2)(C) IN FURTHERANCE OF A VIOLATION OF §2701) (MULTIPLE EMAIL ACCOUNTS); COUNT 2 (VIOLATION OF § 1030(a)(2)(C) IN FURTHERANCE OF A VIOLATION OF § 2701) (MAUREEN ENGER'S EMAIL ACCOUNT); AND COUNT 4 (VIOLATION OF § 1030(a)(2)(C) IN FURTHERANCE OF A VIOLATION OF § 2701) (PATTY FREEMAN'S EMAIL

ACCOUNT) AS A MATTER OF LAW.

A. Congress Did Not Intend to the Defendant's Conduct as Alleged in Counts 1, 2, and 4 to Be Punished as Felony Offenses.

A violation of §1030(a)(2) is generally a misdemeanor. 18 U.S.C. § 1030(c)(2)(A). However, when § 1030(a)(2) is violated "in furtherance of" another crime, it becomes a felony punishable by up to five years imprisonment. 18 U.S.C. § 1030(c)(2)(B)(ii). The Counts 1, 2 and 4 of the Indictment charges violations of § 1030(a)(2), (or a conspiracy to violate § 1030(a)(2), and then seeks a felony enhancement by a violation of § 2701, a statute which prohibits the same conduct as section 1030(a)(2).

When Congress enacted the 1996 amendments to18 U.S.C. § 1030(a) of the Computer Fraud and Abuse Act, P.L.104-292, 110 Stat. 3488, it provided a clear indication of its intention to limit the meaning of the term "for the purpose of committing any criminal or tortious act." That legislative intent is contained in Senate Report (Judiciary Committee) No. 104-357, August 22, 1996, accompanying S. 982.[1]

Senate Report No. 104-357 described the proposed amendments to subsection 1030(a)(2)(C) as "intended to protect against the interstate or foreign theft of information by computer" extending the coverage of § 1030(a)(2) to information held on federal government computers and to computers used in interstate or foreign commerce or communications, if the conduct involved and interstate or foreign communication. (See attached at page 5 of 13). The Senate Report also clarifies the drafters' intention with respect to how the offense is punished. Specifically, the Senate Report states:

---

[1] House Bill H.R. 3623 was passed in lieu of S.1556 and S. 982. History reprinted at 1996 U.S. Code Cong. & Admin. News, p. 4021.

> The seriousness of a breach in confidentiality depends, in considerable part, on the value of the information taken, or what is planned for the information after it is obtained. Thus the statutory penalties are structured to provide that obtaining information of minimal value is only a misdemeanor, but obtaining valuable information, or misusing information in other more serious ways is a felony.[2]
>
> The sentencing scheme for section 1030(a)(2) is part of a broader effort to ensure that sentences for section 1030 violations adequately reflect the nature of the offense. Thus, under the bill, the harshest penalties are reserved for those who obtain classified that could be used to injure the United States or assist a foreign state. Those who improperly use computers to obtain other types of information – such as financial records, nonclassified Government information, and information of nominal value from private individuals or companies – face only misdemeanor penalties, unless the information is used for commercial advantage, private financial gain or to commit any criminal or tortious act.
>
> For example, individuals who intentionally break into, or abuse their authority to use, a computer and thereby obtain information of minimal value of $5,000 or less, would be subject to a misdemeanor penalty. The crime becomes a felony if the offense was committed for purposes of commercial advantage or private financial gain, for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State, or if the value of the information exceeds $5,000.
>
> The terms 'for purposes of commercial advantage or private financial gain' and 'for the purpose of committing any criminal or tortious act' are taken from the copyright statute (17 U.S.C. 506(a)) and the wiretap statute (18 U.S.C. 2511(1)(d)), respectively, and are intended to have the same meaning as in those statutes." (emphasis added).

S.R. 104-357.

Federal courts, including the Fourth Circuit, have frequently interpreted the meaning of the term "for the purpose of committing any criminal or tortious act" in the context of the wiretap statute. In *United States v. Truglio*, 731 F.2d 1123 (4th Cir 1984), the Fourth Circuit

---

[2] Other proposed amendments to section 1030(a) focused on protecting classified national defense or foreign relations information (§1030(a)(1)); providing protection to federal government computers from outside hackers adversely affecting the use of the government's operation of such computer (§1030(a)(3)); accessing a computer with intent to defraud as for example breaking into computers for the purpose of running password cracking programs (§1030(a)(4)); protection from damage to computers (§1030(a)(5));and protection from threats directed against computers.

was required to interpret the breadth of the prohibition against intercepted wire or oral communications and the exception contained in 18 U.S.C. §2511(2) which provides:

> (d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire or oral communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State or for the purpose of committing any other injurious act. (emphasis added).

The court held that the party objecting to the introduction of the intercepted conversation had not met her burden of proving that the tape recordings in that case were made for the purpose of committing a criminal or tortious act. The court pointed specifically to Senator Hart's remarks on the floor of the Congress that §2511(2)(d) was adopted to address situations in which the consenting or intercepting party "acts in any way with the intent to injure the other party to the conversation in any other way. *Id*. at 1131. Accessing an email account for the purpose of accessing an email account does not meet this test.

The Sixth Circuit addressed the issue more directly in *Boddie v. American Broadcasting Companies, Inc.*, 731 F.2d 333 (6th Cir. 1984), cited with approval in the Department of Justice Manual on Prosecuting Network Crimes. In *Boddie*, the court held that the Wiretap Statute requires the plaintiff to show that the defendants intended an illegal, tortious or injurious act other than the recording of the conversation. Specifically, the court stated:

> We agree with the defendants that the court acted properly in excluding from trial plaintiff's allegations that the defendants violated the FCC regulations. The Wiretap Statute requires the plaintiff to show that the defendants intended an illegal, tortious or injurious act other than the recording of the conversations. See *Stamatiou v. United States Gypsum Co.*, 400 F. Supp. 431, 436 n.3 (N.D. Ill. 1975), *aff'd mem*. 534 F.2d 330 (7th Cir. 1976). Even if we assume that the defendants, by the mere interception, violated these regulations, the question remains under §2511(2)(d) whether the defendants intended to use the recorded conversations to injure Boddie. *By-Prod Corp.*

> *v. Armen-Berry*, 668 F.2d 956, 960 (7th Cir. 1982). Thus, the regulations cannot serve as evidence of the defendants' purpose to commit a tortious or injurious act.[3]

Id. at 339. While *Boddie* was on remand, Congress amended §2511(2)(d) deleting the "injurious purpose" language. Under the current version of the statute, nonconsensual interception by a party to a communication is privileged unless the communication is intercepted for a criminal or tortious purpose. Interception for a merely "injurious" purpose is no longer actionable. See Omnibus Crime Control and Safe Streets Act (Title III), 18 U.S. C. §2511 et seq. See also *Boddie v. American Broadcasting Companies, Inc.*, 881 F.2d 267, 268 (1989) (*Boddie II*).[4]

Several courts have held that the mere fact that a defendant violates provisions of federal or state criminal codes which bar wiretapping does not establish a criminal or tortious purpose within the meaning of the Federal Wiretap Statute. See *Vazquez-Santos v. El Mundo Broadcasting Corp.*, 219 F. Supp. 2d 221, 228, 230 (D. Puerto Rico 2002) (holding that violations of Puerto Rico's criminal code prohibiting, *inter alia*, the interception and recording of private communications were insufficient to demonstrate that defendants operated with a

---

[3] The court in *By-Prod Corp. v. Armen-Berry*, 668 F.2d 956, 960 (7th Cir. 1982) held that it was the use of the interception with the intent to harm rather than the fact of interception that is critical to liability under §2511.

[4] The Ninth Circuit previously attempted to address the ambiguity in the term "injurious act" in *Moore v. Telfon Communications Corp.*, 589 F.2d 959, 965-66 (9th Cir. 1978), holding that:

> Congress did not define the meaning of injurious act. While we acknowledge that the term embraces acts not easily classified as either "criminal" or "tortious," we cannot believe that Congress intended it to read to embrace every act which disadvantages the other party to this communication. Such a reading would nullify the exemption created by §2511(2)(a)(d).

purpose to commit a tortious or criminal act other than the interception itself); *Stamatiou v. United States Gypsum Co.*, 400 F. Supp. 431, 436 (1975) (holding that intercepting communications for the purpose of violating the Illinois eavesdropping statute and 47 U.S.C. § 605 (prohibiting the unauthorized publication or use of interstate or foreign communications) does not constitute a violation of §2511.

Congress has thus made clear its intention that the violations of §1030 not be punished as a felony where the crime charged is accessing (or attempting to access) personal email accounts and obtaining (or attempting to obtain) personal email in furtherance of the interception itself, i.e., accessing (or attempting to access) personal email accounts and obtaining (or attempting to obtain) opened or unopened personal email.

B. Punishing Counts 1, 2 and 4 as Felonies Violates the Department of Justice's Policy on Prosecuting Computer Crimes.

The Department of Justice's own manual on prosecuting computer crimes confirms that the criminal or tortious act used to enhance a penalty must be a *separate* act: "Naturally, the 'in furtherance of any criminal or tortious act' language means an act *other than* the unlawful access to stored communications itself." Computer Crime & Intellectual Property Section, U.S. Dep't of Justice, *Prosecuting Computer Crimes* 82 (Feb. 2007) available at http://www.usdoj.gov/criminal/cybercrime/ccmanual/index.html (last visited Oct. 21, 2008) [hereinafter Dep't of Justice, *Computer Crime*] (citing Boddie v. American Broadcasting Co., 731 F.2d 333, 339 (6th Cir. 1984)) (emphasis added).

In addition, the Department notes in its manual that "the 'in furtherance of" language is taken from the Wiretap Act, see 18 U.S.C. § 2511(2)(d), and that at least one appellate court has stated that this enhancement is operative only when a prohibited purpose is the subject's *primary*

motivation or a determinative factor in the subject's motivation. *Id*. at 82 (citing *United States v. Cassiere*, 4 F.3d 1006, 1021 (1st Cir. 1993)). An offender's motivation is not the end of the inquiry: *when* the offender formed the requisite motivation is central to whether the "in furtherance of" enhancement applies. The motivation must have been formed in anticipation of committing the additional crime, and sustained long enough to have caused harm." For example, the manual states, "in *By-Prod Corp. v. Armen-Berry Co*., 668 F.2d 956 (7th Cir. 1982), the Government alleged that the defendant intercepted a telephone call in order to "commit an act that is criminal or tortious under federal or state law." *Id*. The Seventh Circuit held that even if the Defendant formed the requisite intent to use the intercepted tape recording, his failure to actually use the recording was what mattered, because his wrongful intention was not sustained.

> We doubt [] that a tape recording which was never used could form the basis for liability . . . . It would be a dryly literal reading of the statute that found a violation because at the moment of pressing the "on" button a party to a conversation conceived an evil purpose though two seconds later he pressed the "off" button and promptly erased the two seconds of tape without even playing it back. **A statute that provides for minimum damages of $1000 per violation must have more substantial objects in view than punishing evil purposes so divorced from any possibility of actual harm**.

Id. at 959-60 (emphasis added). See also *Stockler v. Garrett*, 893 F.2d 856 (6th Cir. 1990) (holding that 'interception' and not 'use' is all that is required to violate Wiretap Act, but failing to abrogate Boddie's holding that the criminal or tortious purpose must be 'other than" the interception and/or use).'"

Accordingly, for the reasons contained in the Department of Justice's own policies, the felony enhancement must be dismissed.

CONCLUSUION

In addition to protecting against subsequent prosecutions for the same offense, the Double Jeopardy Clause protects against multiple punishments for the same offense. *North Carolina v. Pearce*, 395 U.S. 711, 717 (1969); U.S. Const. amend. V. By extension, the Double Jeopardy Clause protects against duplicitous and enhanced punishments for the same offense. The mere fact that two convictions are authorized by different statutory provisions does not establish clear legislative intent that Congress specifically authorized cumulative punishment for the same conduct. See *Rutledge v. United States*, 517 U.S. 292 (1996); *Williams v. Singletary*, 78 F.3d 1510 (11th Cir. 1996) (no clear indication of legislative intent to authorize cumulative conviction and sentences because no clear language in statute and no indication from state courts or legislature as to how to interpret state law).

For the reasons stated, the felony enhancements in Counts 1, 2, and 4 should be dismissed as a matter of law.

Respectfully submitted,

ELAINE ROBERTSON CIONI
By Counsel

/s/

Nina J. Ginsberg, Esquire
VSB # 19472
Counsel for Elaine Robertson Cioni
DiMuroGinsberg, P.C.
908 King Street, Suite 200
Alexandria, VA 22314
Phone: 703-684-4333
Fax: 703-548-3181
nginsberg@dimuro.com

CERTIFICATE OF SERVICE

I hereby certify that on December 11, 2008, I will electronically file the foregoing pleading with the Clerk of Court using the CM/ECF system, which will then send a notification

of such filing (NEF) to:

Jay Prabhu, Esquire
Assistant U.S. Attorney
2100 Jamieson Avenue
Alexandria, VA 22314
703-299-3700
jay.prabhu@usdoj.gov

/s/
Nina J. Ginsberg, Esquire
VSB # 19472
Counsel for Elaine Robertson Cioni
DiMuroGinsberg, P.C.
908 King Street, Suite 200
Alexandria, VA 22314
Phone: 703-684-4333
Fax: 703-548-3181
nginsberg@dimuro.com